SUCCESS STORY

flare

Managed Security Service Provider reduces dark web investigation time by 10x

The customer

Leading Managed Security Service Provider

Covering **North America** and **Europe**

They offer:

- Risk assessment
- Penetration testing
- Incident response
- Post-breach remediation support
- Ongoing security posture monitoring

The Challenges

Most managed security service providers (MSSP) are looking for ways to expand the variety of services that they can offer to their clients. One potential service that MSSPs can provide is the ability to monitor the dark web. However, MSSPs face two main challenges.

1. Dark Web Monitoring Requires Additional Knowledge

There is a lack of experience in the cybersecurity space when it comes to dark web monitoring. The security professionals in the space don't always have strong enough knowledge of the cybercriminal underground to keep up with the pace at which new dark web sources spring up.

2. Dark Web Monitoring Takes Time

MSSP employees who have dark web monitoring experience face the time required to monitor the dark web as an additional challenge. It takes an extended period to manually create accounts (that often get banned), pay fees in Bitcoin to access some sites and use deprecated search bars in other sites. Additionally, various other hurdles make the economics of offering this service to customers hard to justify.

Choosing Flare

It only took a few days of using Flare for a senior penetration tester to realize the value Flare could bring to his company. Prior to Flare this customer had tried competing products for 6 months without finding much actionable information. A two week trial with Flare is all that was needed to uncover high fidelity and actionable findings on behalf of his client.

Trusting Flare's 3 layers approach to Dark web coverage

The Flare team has taken dark web monitoring very seriously ever since the company's first days. Our dark web monitoring approach consists of three complementary components that ensure that our data is accurate, up to date, and is keeping up with new dark web platforms. First is the research and threat hunting team that follows trends and news on upcoming illicit websites.

Second is our technical team that adds new data sources to our collection engine. Lastly, our automated collection engine crawls every source every day, saves the results in our local databases, and archives dark web posts and platforms. Customers can take advantage of our three-factor approach and easily query any data that they require.

Benefits

Save time and cover more

The senior penetration tester was not only saving time in orders of manitudes, but was also converin gmuch more of th erelevant sections of the dark web.

Upskill you team on dark web monitoring

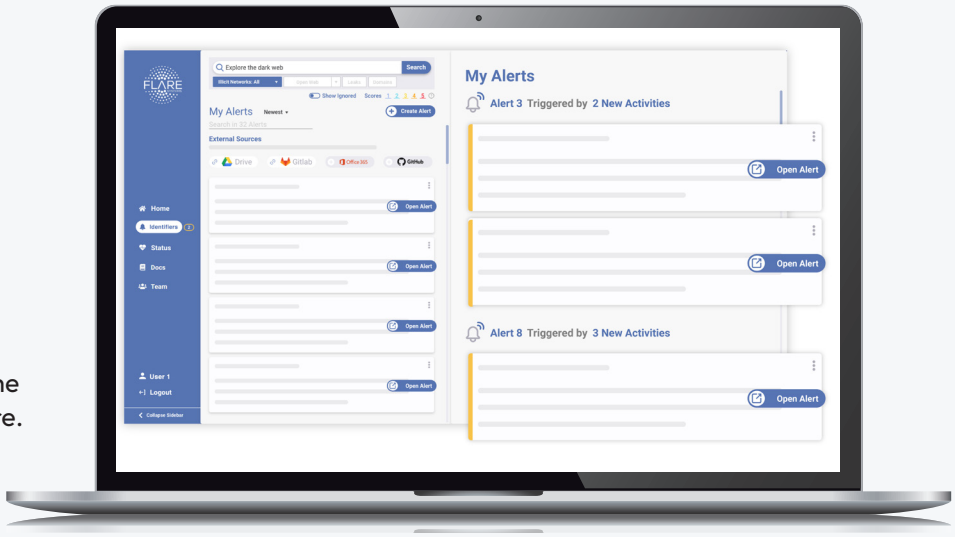
In addition, the ease of use of Flare allowed him to delegate the initial dark web data discovery part to team members with close to no experience with the dark web. Having more hands on deck to support dark web investigation assignments allowed the senior penetration tester's team to offer dark web assessments and monitoring to an increasing number of their customers, generating more revenue for his firm.

> "What used to take about 1500 hours to complete can now be done in 1 week."
>
> -Senior security specialist, North American MSSP

> "Flare allows me to empower junior analysts to do dark web investigations that were previously impossible, hence liberating bandwidth."
>
> -Senior security specialist, North American MSSP

Product Highlights

- Onboard and empower your existing team in a matter of hours
- Bringing context to an alert helps
- Higher-risk alerts are managed quickly thanks to the unique scoring system of Flare.



Learn more about our solution →

Request a Demo

flare

flare.systems

hello@flaresystems.com